Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Ville Vaittinen

Yrityksen kameravalvontajärjestelmien runkoverkon arkkitehtuurisuunnittelu

Metropolia Ammattikorkeakoulu

Tekniikan ammattikorkeakoulututkinto

Tietotekniikan koulutusohjelma

Insinöörityö

13.9.2018

Tekijä Otsikko Sivumäärä Aika	Ville Vaittinen Yrityksen kameravalvontajärjestelmien runkoverkon arkkitehtuurisuunnittelu 31 sivua + 2 liitettä 13.9.2018
Tutkinto	Insinööri AMK
Tutkinto-ohjelma	Tietotekniikan koulutusohjelma
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Kehityspäällikkö Tiina Korhonen Ryhmäpäällikkö Panu Oksman Osaamisaluepäällikkö Janne Salonen

Tässä energia-alan yritykselle tehdyssä insinöörityössä selvitettiin, minkälainen kameravalvontajärjestelmien runkoverkko yrityksen pitäisi toteuttaa, jotta se voisi siirtää kameravalvontajärjestelmät toimistoverkosta ja prosessiverkosta uuteen verkkoalueeseen. Uusi runkoverkko pitäisi suunnitella siten, että siinä ei olisi nykyisen verkkoarkkitehtuurin haasteita.

Selvitystyön pohjaksi insinöörityössä selvitettiin nykyisten järjestelmien tietoliikennetekninen liityntätapa sekä yrityksen verkkoarkkitehtuuri ja tietoturvavaatimukset. Selvitystyön aikaiseen verkkoarkkitehtuuriin liittyi rajoituksia, minkä vuoksi kameravalvontajärjestelmiä ei voitu käyttää mahdollisimman tehokkaasti. Myös lainsäädännön vaikutuksia suunnittelutyöhön arvioitiin.

Selvityksen pohjalta kameravalvontajärjestelmiä varten suunniteltiin uusi runkoverkko, jossa ei olisi selvityksessä tunnistettuja rajoituksia. Verkkosuunnittelussa otettiin kantaa verkon tietoliikennearkkitehtuuriin, tietoliikenteen suodatukseen ja eristämiseen sekä kameravalvontajärjestelmien liityntään. Työssä vertailtiin ja valittiin kytkinmalli, jolla runkoverkko voidaan toteuttaa.

Runkoverkko suunniteltiin rengastyyppiseksi, jossa kytkimet ovat niin sanottuja modulaarisia kytkimiä. Modulaarisessa kytkimessä on moduulipaikat, joihin asennetaan liityntäkohtaisesti sopivat moduulit. Rengasverkko suunniteltiin siten, että se toteutetaan vain kolmella kytkimellä, koska yrityksen olemassa oleva valokuituverkko on niin laaja, että eri kohteiden kameravalvontajärjestelmät voidaan tuoda näihin kolmeen kytkimeen valokuitu-ethernet-muuntimilla.

Työn liitteet julistettiin salaisiksi, koska ne sisältävät yrityksen tietoturvaperiaatteiden mukaan salassa pidettävää tietoa.

Avainsanat	Tietoliikenne, kameravalvonta, verkko, prosessiverkko

Author Title	Ville Vaittinen Network architecture design of backbone network for corporate camera surveillance systems
Number of Pages Date	31 pages + 2 appendices 13 Sep 2018
Degree	Bachelor of Engineering
Degree Programme	Degree Programme in Information and Communications Technology
Specialisation option	Networks
Instructor(s)	Kehityspäällikkö Tiina Korhonen Ryhmäpäällikkö Panu Oksman Osaamisaluepäällikkö Janne Salonen

This bachelor's thesis is made for energy company to explore what kind of camera surveillance system backbone network the company should implement so they can move camera surveillance systems from the office network and process network to a new network that does not face the current network architecture challenges.

As a basis for the study the current network architecture and connection methods of camera surveillance systems were explored, as well as company own security requirements and regulations about network design solutions.

Based on the survey a new backbone network was designed for camera surveillance systems where there would not be any identified restrictions. The network design included a network architecture, data filtering and isolation as well as connection of camera surveillance systems. In the study network switch models were compared and a suitable model was found.

The backbone network was designed as a ring type where switches are so-called modular switches. The modular switches have modular slots where modules are selected for the connection. The ring network was designed to be implemented with only three network switches because the company's existing fiber optic network is so extensive that camera surveillance systems from different locations can be connected to these three switches with optical fiber-ethernet converters.

The attachments about this thesis were declared secret as they contain confidential information in accordance with the company's security principles.

Keywords	Communication, camera surveillance, network, process network

Sisällys

Lyhenteet

BUM	Broadcast unicast multicast. Yleinen nimitys broadcast-, unicast- ja multicast-tietoliikenteestä.
DMZ	Demilitarized zone. Demilitarisoitu alue on lähiverkon osa, joka yhdistää turvallisen ja turvattoman verkon toisiinsa.
DVR	Digital video recorder. Digitaalinen videotallennin.
FTP	File transfer protocol. Tiedonsiirtomenetelmä.
Gb	Gigabitti. Miljardi bittiä.
Gbps	Gigabittiä sekunnissa. Miljardi bittiä sekunnissa.
GDPR	General Data Protection Regulation. Yleinen tietosuoja-asetus.
GE	Gigabit ethernet. Nopeudeltaan yhden gigabitin ethernet-yhteys.
H.264	Videopakkausstandardi.
ICT	information and communications technology. Tieto- ja viestintäteknologia.
IEEE	Institute of Electrical and Electronics Engineers. Kansainvälinen tekniikan alan järjestö.
IP	Internet Protocol. Internetprotokolla.
IT	Information technology. Informaatioteknologia.
JPEG	Joint Photographic Experts Group. Kuvanpakkaus- ja tallennusformaatti.
L2	Layer 2. OSI-mallin taso 2, siirtokerros.
L3	Layer 3. OSI-mallin taso 3, verkkokerros.

LASER	Light Amplification by Stimulated Emission of Radiation. Laite joka tuottaa koherenttia valoa.
LED	Light-Emitting Diode. Valodiodi.
Mb	Megabitti. Miljoona bittiä.
Mbps	Megabit per second. Miljoona bittiä sekunnissa.
MPEG	Moving Picture Experts Group. Kuvanpakkausstandardi.
NMS	Network management system. Tietoliikenneverkon hallintajärjestelmä.
NVR	Network video recorder. Lähiverkkoon kytketty videopalvelin.
OSPF	Open Shortest Path First. Reititysprotokolla.
OT	Operational technology. Tietojärjestelmät joilla on fyysinen liityntäpinta, esimerkiksi teollisuusautomaatio.
PVST+	Per-VLAN Spanning Tree Plus. Layer2-verkonhallintaprotokolla.
RF	Radio frequency. Radiotaajuus.
SaaS	Software as a service. Sovelluksen tai järjestelmän hankkiminen palveluna.
SFP	small form-factor pluggable. Tietoliikennelaitteen moduuli.
SNMP	Simple Network Management Protocol. Tietoliikenneverkkojen hallintaprotokolla.
SSH	Secure shell. Salattuun tietoliikenteeseen tarkoitettu ohjelma.
TCP/IP	Transmission Control Protocol / Internet Protocol. Kokoelma tietoliikenneprotokollia.
WDM	Wavelength-division multiplexing. Aallonpituuskanavointi.

WiFi	Langaton lähiverkko.
VLAN	Virtual local area network. Virtuaalilähiverkko.

1 Johdanto

Tässä insinöörityössä suunnitellaan erään energia-alan yrityksen kameravalvontajärjestelmille runkoverkko sekä järjestelmien liityntätavat uuteen verkkoon. Lisäksi suunnitellaan ja kuvataan järjestelmien etäkäyttö- ja tiedonsiirtotavat. Kameravalvontajärjestelmien tehokkaan etäkäytön, tietoturvan ja kustannustehokkuuden vuoksi kohdeyrityksellä on tarve hankkia keskitetty tietoliikenneratkaisu nykyisen hallitsemattomasti rakentuneen arkkitehtuurin tilalle. Kohdeyrityksen kamerajärjestelmät on sijoitettu yrityksen toimistoverkkoon sekä suljettuun prosessiverkkoon.

Insinöörityö pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

1. Minkälaisia kameravalvontajärjestelmiä yrityksellä on käytössä tällä hetkellä ja miten ne on kytketty muihin tietoverkkoihin?

2. Minkälainen runkoverkko yrityksen tulisi rakentaa, jotta siihen voitaisiin liitää tietoturvallisesti ja kustannustehokkaasti yrityksen nykyiset kameravalvontajärjestelmät?

Suunnittelutyön pohjaksi laaditaan nykytilan kuvaus sekä selvitys käytössä olevista kamerajärjestelmistä. Nykytilan kuvauksen pohjalta tehdään uuden runkoverkon tietoliikennearkkitehtuurisuunnitelma.

Työn tuotoksena kohdeyritys saa tämän insinöörityön, jonka kirjallisessa osuudessa sekä liitteissä on esitetty kameravalvontajärjestelmien uuden runkoverkon tietoliikennetekninen toteutussuunnitelma sekä pohjatiedot kameravalvontajärjestelmien siirtoprojektia varten.

2 Kameravalvontajärjestelmät yleisesti

Tässä luvussa avataan yleisellä tasolla kameravalvontajärjestelmien tarkoitus, käyttöä yrityksissä, teknistä toimintaa ja lainsäädäntöä.

2.1 Kameravalvontajärjestelmät

Kameravalvontajärjestelmät ovat laajalti käytettyjä järjestelmiä, joilla yritykset, yhteisöt ja viranomaiset tuottavat ja tallentavat kuvallista informaatiota tiloista, kiinteistöistä ja alueista osana toimitilaturvallisuuden toteuttamista. Näissä käyttötapauksissa kameravalvonnalla pyritään estämään mahdolliset ongelmat sekä selvittämään jo syntyneitä ongelmia.

Toimitilaturvallisuuden lisäksi kameravalvontajärjestelmiä käytetään paljon myös muissa käyttötarkoituksissa kuten teollisuudessa ja sairaanhoidossa. Kameravalvonnat sopivat muun muassa prosessien valvontaan sekä henkilö- ja liikennevalvontaan yrityksissä ja viranomaisilla. [Sallinen 2011: 1.]

Kameravalvontajärjestelmissä käytetään joko analogi- tai digitalitekniikkaa. Analogisessa järjestelmässä kamerana on analogikamera, jonka tuottama analoginen kuvavirta siirretään joko analogiselle valvontamonitorille ja/tai videotallentimelle. Videotallennin tallentaa kuvavirran nauhalle tai digitalisen muunnoksen jälkeen sähköiseen muistiin. Analogisista videotallentimista käytetään nimitystä DVR (digital video recorder). DVR-tallentimen toiminta perustuu kuvankaappauskorttiin, kuvan tallennukseen sekä katseluohjelmistoon tai monitoriin. DVR-laite voi olla myös kytketty lähiverkkoon, jolloin kuvankaappauskortin kautta kerättyjä videokuvia voi katsoa PC:llä reaaliaikaisesti tai tallentimen muistista.

Digitalisessa järjestelmässä digitaalinen kamera lähettää tietoliikenneverkon kautta TCP/IP-protokollapinossa kulkevaa digitalista kuvadataa. [Real time streaming protocol 1998: 2.]

Data tallennetaan videopalvelimelle, jota kutsutaan NVR-laitteeksi (network video recorder). Videopalvelimeen käyttö tapahtuu tietoliikenneverkon kautta joko selaimella tai erityisellä katseluohjelmistolla, johon on usein mahdollista liittää myös käyttäjätunnistus ja käyttöoikeuksien hallinta. Kuvaa voidaan siirtää ja tallettaa verkon kautta myös muihin videopalvelimiin.

Kuvadataa voidaan siirtää kameralta DVR- tai NVR-laitteelle sekä langallisesti että langattomasti. Langattomat yhteydet ovat digitaalisessa kuvadatassa yleensä WiFi-verkkoja tai mobiiliyhteyksiä. Analogitekniikassa käytetään RF-lähetintä ja vastaanotinta.

2.2 Kameravalvontajärjestelmät yrityksissä

Yritysturvallisuuden toteuttamisessa on tärkeää erilaisten riskien tunnistaminen ja niiden hallinta. Osana yritysturvallisuuden turvallisuustyötä yritykset voivat hankkia teknisiä apujärjestelmiä varmistaakseen liiketoiminnan häiriöttömän jatkumisen. Oikein toteutetuilla turvajärjestelmillä voidaan ennaltaehkäistä erilaisia onnettomuus- ja vaaratilanteita kuten myös vahinkoja ja rikollista toimintaa. Kulunvalvonta ja murtovalvonta yhdessä kameravalvonnan kanssa tarjoavat kattavat työkalut yrityksen turvallisuustyöhön. [Sallinen 2011: 1.]

Kameravalvontajärjestelmien käyttömahdollisuudet laajenevat teknologian ja ohjelmistojen kehittyessä. Automaatio, koneoppiminen ja muut prosessit, joissa tarvitaan kuvantunnistusta sekä visuaalista päätöksentekoa kehittyvät koko ajan tuoden kameravalvontajärjestelmille uusia käyttökohteita. [Kiesiläinen 2016: 3.]

Kuten kaikista järjestelmistä, myös kameravalvontajärjestelmiä voi hankkia pilvipalveluna (SaaS) tai asiakkaan omaan ympäristöön asennettuna (on-demand) ratkaisuna. Yrityksen tulee valita itselleen sopiva ratkaisu riskiarvion pohjalta. Esimerkiksi etätoimipisteen kameravalvonta saattaa olla mahdollista toteuttaa pilvipalveluna, mutta tehtaan tuotantoprosessia valvova järjestelmää ei voisi riskiarvion pohjalta toteuttaa sillä riskillä, että tehtaan internetyhteys ei toimi, mikä aiheuttaa järjestelmälle epäkäytettävyyttä.

2.3 Kameravalvontajärjestelmät ja lainsäädäntö

Kameravalvonnasta, järjestelmien käytöstä ja tietojen käsittelystä on säädetty seuraavissa laeissa:

- rikoslaki
- laki yksityisistä turvallisuuspalveluista
- laki yksityisyyden suojasta työelämässä
- laki yhteistoiminnasta yrityksessä
- henkilötietolaki

- työturvallisuuslaki. [Sallinen 2011: 1.]

Lisäksi EU:n yleisessä tietosuoja-asetuksessa (GDPR) säädetään kansalaisten oikeuksista sekä henkilötietojen käsittelystä. [Usein kysyttyä EU:n tietosuoja-asetuksesta. 2018: 4.] Näiden lakien keskeisimmät kohdat kameravalvonnan suhteen on kuvattu seuraavissa lakikohtaisissa luvuissa.

2.3.1 Rikoslaki

Rikoslaissa säädetään välillisesti kameravalvontaan liittyen salakatselusta sekä yksityiselämää loukkaavan tiedon levittämisestä. Rikoslain 24. luvun 6 §:ssä (9.6.2000/531) säädetään salakatselusta seuraavasti: ”Joka oikeudettomasti teknisellä laitteella katselee tai kuvaa 1) kotirauhan suojaamassa paikassa taikka käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaa henkilöä taikka 2) yleisöltä suljetussa 3 §:ssä tarkoitetussa rakennuksessa, huoneistossa tai aidatulla piha-alueella oleskelevaa henkilöä tämän yksityisyyttä loukaten…”.

Yksityiselämää loukkaavan tiedon levittämistä säädetään rikoslain 24 luvun 8 §:ssä ”Joka oikeudettomasti 1) joukkotiedotusvälinettä käyttämällä tai 2) muuten toimittamalla lukuisten ihmisten saataville - esittää toisen yksityiselämästä tiedon, vihjauksen tai kuvan siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa, on tuomittava yksityiselämää loukkaavasta tiedon levittämisestä sakkoon...”

Salakatselu ja yksityiselämää loukkaavan tiedon levittäminen on otettava huomioon kameravalvontajärjestelmien suunnittelussa ja toteutuksessa kuten myös järjestelmien käyttäjien koulutuksessa. Tietoliikenteen toteutukseen rikoslaissa säädetyt asiat eivät vaikuta.

2.3.2 Laki yksityisistä turvallisuuspalveluista

Laki yksityisistä turvallisuuspalveluista (21.8.2015/1085) käsittelee vartioimisliiketoimintaa ja turvasuojaustoimintaa. Kameravalvontaan liittyen laissa käsitellään järjestelmien suunnittelun, asennuksen ja työnjohdon luvanvaraisuutta, valvonnassa syntyvien henkilötietojen käsittelyä sekä salassapitovelvollisuutta.

2.3.3 Laki yksityisyyden suojasta työelämässä

Laki yksityisyyden suojasta työelämässä määrittelee, miten ja mihin tarkoituksiin kameravalvontaa saa käyttää työpaikalla ja työelämässä. Laissa määritellään myös tallenteiden enimmäissäilytysajat. Kameravalvontajärjestelmien runkoverkon toteutukseen kyseinen laki ei vaikuta. [Laki yksityisyyden suojasta työelämässä 759/2004: 5.]

2.3.4 Laki yhteistoiminnasta yrityksissä

Yhteistoimintalaissa säädetään, miten työnantajan on käsiteltävä yhteistoimintamenettelyissä työntekijöihin kohdistuvan kameravalvonnalla toteutettavan valvonnan tarkoitus ja toteutus [Laki yhteistoiminnasta yrityksissä 334/2007]. Oman arvioni mukaan yhteistoimintakäsittelyä ei tarvita kameravalvontajärjestelmien runkoverkon käyttöönotossa, mutta asia on hyvä selvittää yrityksessä ennen verkon toteutusta.

2.3.5 Työturvallisuuslaki

Työturvallisuuslaissa säädetään työturvallisuuteen liittyviä asioita, kuten miten väkivallan uhkaan työpaikalla tulee varautua ja miten sitä voidaan torjua sekä millaisia toimia ja järjestelyjä työpaikalla tulee järjestää. Lisäksi laista voidaan johtaa johtopäätöksenä, että kameravalvontaa voidaan pitää yhtenä työturvallisuuteen liittyvänä järjestelmänä. Kohdeyrityksessä, jossa kameravalvonnalla valvotaan myös tuotantoprosessitiloja, voi kameravalvonnan tuottama kuva toimita päätöksenteon tukena, kun työntekijä harkitsee kulkemisen turvallisuutta kyseiseen tilaan.

Yritys on vastuussa kameravalvontajärjestelmien toiminnasta ja kunnossapidosta. Finanssialan kameravalvontaoppaan mukaan kameravalvontajärjestelmien huollon laiminlyöminen voisi johtaa tuomioon työturvallisuusrikoksesta. [Sallinen 2011: 1.] Tästä voidaan tehdä johtopäätös, että myös kameravalvontajärjestelmien runkoverkko on yksi keskeinen komponentti yrityksen työturvallisuuden järjestämisessä ja sen kunnossapidolla on suuri merkitys.

2.3.6 Henkilötietolaki

Henkilötietolaissa säädetään, miten ja milloin henkilötietoja saa kerätä, miten niitä käsitellään ja mitä vaatimuksia henkilötietorekisterien pitoon liittyy. Tietosuojavaltuutetun toimiston mukaan kameravalvontajärjestelmä muodostama ääni ja kuva ovat henkilötietolaissa rinnastettavaa henkilötietoa vain, jos ne tallennetaan. Näin ollen kameravalvontajärjestelmien kautta tapahtuu henkilötietojen käsittelyä vain, jos etäkäytetään kameratallentimia ja katsellaan näiden tallentamaa informaatiota.

2.3.7 Yleinen tietosuoja-asetus

Yleinen tietosuoja-asetus eli yleisemmin GDPR (General Data Protection Regulation) on henkilötietojen käsittelyä sääntelevä laki, jonka soveltaminen alkoi 25.5.2018. Tietosuojavaltuutetun toimiston mukaan lain tavoitteena on parantaa henkilötietojen suojaa ja tietosuojaoikeuksia, vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa ja edistää digitaalisten sisämarkkinoiden kehittymistä. [Usein kysyttyä EU:n tietosuoja-asetuksesta 2018: 4.]

Yleinen tietosuoja-asetus ei erityisesti laajenna Suomen henkilötietolain määritelmää henkilötiedoista, mutta kameravalvontajärjestelmien runkoverkon ylläpidon ja ICT-tuotannon näkökulmasta se määrittelee ilmoitusvelvollisuuden tietoturvaloukkauksissa. [Mikä on tietoturvaloukkaus ja miten sellaisen sattuessa pitää toimia? 2018: 7.]

3 Kohdeyrityksen kameravalvontajärjestelmien nykytilan kuvaus

Tässä luvussa kerrotaan kohdeyrityksen käyttämistä kamerajärjestelmistä sekä verkkoarkkitehtuurista kuten myös yrityksen liiketoimintatarpeista ja prosesseista, joita varten järjestelmät on hankittu.

3.1 Kohdeyritys

Yritys, jolle tämä insinöörityö tehdään, on suuri energia-alalla toimiva yritys, jonka liiketoimintaan kuuluu sähkön, kaukolämmön sekä kaukokylmän tuotanto ja jakelu. Lisäksi yrityksellä on muita tuotteita sekä digitalisia palveluita.

Yrityksellä on perinteisiä toimistotiloja, joihin ei kohdistu erityisiä toimialalta poikkeavia riskejä. Toimistotilojen isäksi yrityksellä on kymmeniä teollisuuskohteita kuten voimalaitoksia, lämpölaitoksia, sähköasemia ja pumppuasemia. Lisäksi yritys vastaa useiden maanalaisten yhteiskäyttötilojen turvallisuudesta, mikä sisältää myös tilojen kameravalvonnan toteutuksen.

Voima- ja lämpölaitoksilla kameravalvontaa tarvitaan perinteiseen aluevalvontaan, kuten ulkoalueiden ja sisätilojen turvallisuusvalvontaan. Perinteisen aluevalvonnan lisäksi kameravalvontaa käytetään prosessitilojen ja prosessien valvontaan. Kameravalvonta tehostaa tuotantoprosessien valvontaa, kun samalla henkilöstömäärä pystytään valvomaan samanaikaisesti laajempaa aluetta. Kameravalvonta parantaa myös henkilöturvallisuutta, kun vaarallisia painelaitteita ja polttoaineen kuljettimia voidaan valvoa etäältä. Painelaitteet kuten kattilat, putket ja pumput voivat vikaantuessaan aiheuttaa vakavia henkilövahinkoja, jotka on mahdollista välttää etävalvonnalla.

Yrityksellä on käytössä konenäkösovellus automaattisessa ulkovalvonnassa, jossa tunnistetaan rekisterinumerot kameran kuvavirrasta. Yrityksen avainhenkilöiden kanssa käytyjen keskustelujen mukaan konenäöllä on paljon kehityspotentiaalia yrityksen teollisuusprosessien valvonnassa, koska sillä voitaisiin tunnistaa esimerkiksi vuotavia putkia ja venttiileitä.

3.2 Huoltovarmuus

Huoltovarmuudella tarkoitetaan yhteiskunnan kykyä ylläpitää sellaiset perustoiminnot, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä kuten myös poikkeusoloissa. [Mitä on huoltovarmuus? 2018: 8.]

Koska kohdeyritys toimii energia-alalla, luetaan se valtioneuvoston 5.12.2013 päätöksen mukaisesti huoltovarmuuskriittiseksi toimijaksi. Päätöksen mukaan seuraavat toimialat ovat huoltovarmuuskriittisiä:

- energian tuotanto, siirto- ja jakeluverkot
- tieto- ja viestintäjärjestelmät, -verkot ja -palvelut

- finanssialan palvelut
- liikenne ja logistiikka
- vesihuolto
- infrastruktuurin rakentaminen ja kunnossapito
- jätehuolto erityistilanteissa. [Tavoitteet 2018: 9.]

Yritys vastaa sekä sähkön tuotannosta että jakelusta kuten myös kaukolämmön tuotannosta ja siirrosta, joten se on erittäin keskeisessä asemassa huoltovarmuuden toteutuksessa.

Kameravalvontajärjestelmillä toteutetaan yritysturvallisuutta ja valvotaan tuotantoprosessia, mikä tekee siitä osan huoltovarmuusketjua, jonka yrityksen eri toiminnot ja järjestelmät muodostavat.

3.3 Yrityksen ICT-tuotanto

Yrityksen ICT-palvelutuotannosta vastaa IT-kokonaispalvelutoimittaja, jonka vastuulle kuuluu ICT-infran ylläpito ja hallinnointi. ICT-infra käsittää datakeskukset, palvelimet, tallennusratkaisut, tietoliikenteen kytkinverkot ja palomuurit.

Yrityksen oma ICT omistaa fyysiset tietoliikenneyhteydet, sekä myös vastaa yhteyksiin tehtävistä muutoksista. Yrityksellä on valokuitu- ja kupariyhteysverkko, joka kattaa kaikki toimipisteet sekä prosessitilat.

Kameravalvontajärjestelmät ovat liiketoimintojen vastuulla ja omistuksessa. Yrityksen ICT tarjoaa näille tietoliikenneyhteydet ja on mukana järjestelmien elinkaarenhallinnassa.

3.4 IT / OT -jako

Yrityksessä tietojärjestelmät jaetaan Gartnerin IT- ja OT-alueen välillä. IT-alueen (informational technology) järjestelmät ovat perinteisiä yrityksen IT-järjestelmiä, kuten sähköpostijärjestelmät, taloushallinto ja henkilöstöhallinnon järjestelmiä. OT-alueen (operational technology) järjestelmillä tarkoitetaan järjestelmiä, joilla on jokin fyysinen liityntärajapinta mittareihin, antureihin tai toimilaitteisiin. [Operational Technology (OT) 2018: 10.]

Yrityksen ohjeistuksen mukaan OT-alueetta ovat energian tuotantoon, hankintaan, siirtoon ja jakeluun liittyvät energian hallinta-, kunnonvalvonta-, automaatio- ja kaukokäyttöjärjestelmät. Alueeseen sisältyvät näiden ala-asemat ja tietoliikenneratkaisut palveluineen. Myös kiinteistöjen kunnon-, kulun- ja turvallisuuden valvontajärjestelmät kuuluvat alueeseen. Etäluettaviin ja ohjattaviin energianmittauksiin sekä ulkovalaistuksen ohjaukseen liittyvät järjestelmät ovat myös OT-aluetta. [Yrityksen prosessitietojärjestelmiä koskeva konserniohje: 11.]

3.5 Yleinen tietoverkkoarkkitehtuuri suurissa ja keskisuurissa yrityksissä

Suurissa ja keskisuurissa yrityksissä tietoliikenneverkko muodostuu tyypillisesti toiminnallisista kerroksista, jotka ovat liityntäkerros, jakelukerros sekä ydinkerros.

Liityntäkerros on tarkoitettu lähinnä loppukäyttäjiä tai prosessiverkkotapauksessa kenttälaitteita varten, jotka liittyvät kytkimiin tietoliikenneyleiskaapeloinnin kautta. Tällä tasolla käytetään tyypillisesti ethernet-kaapeleita, mutta erikoistapauksissa kuten prosessiverkkokäytössä myös optiset kaapelit saattavat tulla kyseeseen. Liityntäkerroksen kytkimiä kutsutaan myös reunakytkimiksi. Liityntäkerroksen laitteet ovat tyypillisesti OSI-mallin L2-tason laitteita, joissa ei ole esimerkiksi tietoliikenteen suodatusta tai reititystä. Liityntäkerroksen laitteet voidaan suunnitella esimerkiksi osasto-, kerros- tai porraskäytäväkohtaisiksi.

Liityntäkerroksen laitteet kytketään jakelukerroksen kytkinlaitteisiin, jotka keräävät toimipisteen liityntäkerroksen yhteydet usein vikasietoisiin ja kahdennettuihin L2- tai L3-tason laitteisiin. Jakelukerroksen tasolla on usein tarpeen toteuttaa reititystä, jotta liityntäkerrokset eivät muodosta liian laajoja alueita, jolloin esimerkiksi L2-tason BUM-liikenne le-

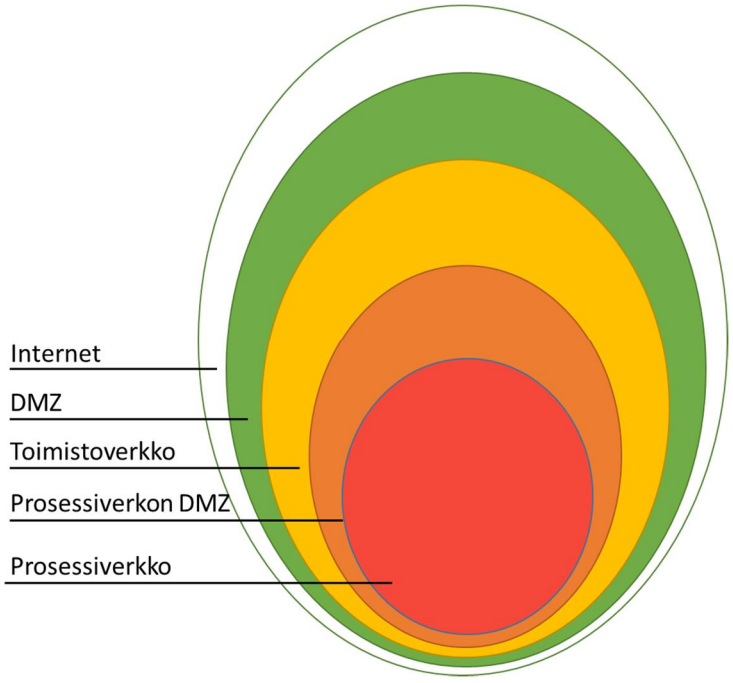
viäisi turhan laajalle rasittaen verkkoa. BUM-liikenne on verkon aktiivi- ja asiakaslaitteiden tuottamaa broadcast-, unicast- ja multicast-liikennettä. Liityntäkerroksella käytetään tyypillisesti optisia kaapeleita.

Jakelukerroksen laitteet kytketään ydinkerrokseen, jolla kytketään ja reititetään jakelukerroksilta tulevaa liikennettä keskenään ja internetin välillä. Verkon tietoliikennettä suodatetaan palomuureilla, yleensä ydintasolla mutta joskus myös jakelutasolla. [Hakala, Vainio 2005: 12.]

3.6 Kohdeyrityksen tietoliikenneverkkoarkkitehtuuri

Yrityksen tietoliikenneverkot on jaettu viiteen hallinnolliseen alueeseen, jotka ovat DMZ, toimistoverkko, prosessiverkon väliverkko, prosessiverkko ja asiakasverkot. Järjestelmät sijoitetaan käyttötarkoituksen ja luokittelun perusteella valittavaan verkkoon.

Tällä jaolla aikaansaadaan niin sanottu sipulisuojaus, jossa julkiset internetiin tarkoitetut palvelut ovat ulommilla verkkoalueilla ja tarkemmin suojeltavat sisäiset järjestelmät sisemmillä vyöhykkeillä. Nimitys sipulimalli, jota kutsutaan myös syvyyssuojaukseksi, tulee verkkojen sisäkkäisestä esitystavasta, mikä muistuttaa sipulia. Esitystapa on kuvattu kuvassa 1.



Kuva 1. Verkon syvyyssuojaus.

IT-järjestelmät sijoitetaan toimistoverkkoon ja OT-järjestelmät prosessiverkkoihin. Historiasyistä joitain yrityksen OT-järjestelmiä on yhä toimistoverkossa, mutta tavoitteena on siirtää ne kaikki prosessiverkon puolelle. Tämä selvitys osaltaan edistää tätä tavoitetta.

Verkot ja niiden käyttötarkoitukset kuvataan seuraavissa verkkokohtaisissa luvuissa.

3.6.1 DMZ

DMZ-verkko on edustaverkko toimistoverkon ja internetin välissä. DMZ tulee englannin kielen sanoista demilitarized zone. DMZ:lle sijoitetaan internetpalveluiden palvelimet kuten WWW-palvelimet sekä integraatiopalvelimet, ja sen tarkoituksena on suojata sisempiä verkkoalueita tuomalla yksi verkkokerros lisää luotetun ja epäluotetun verkkoalueen välille. [Demilitarisoitu alue 2018: 13.] DMZ-palvelimet ovat tyypillisesti sellaisia, jotka tarjoavat palveluita internettiin.

3.6.2 Toimistoverkko

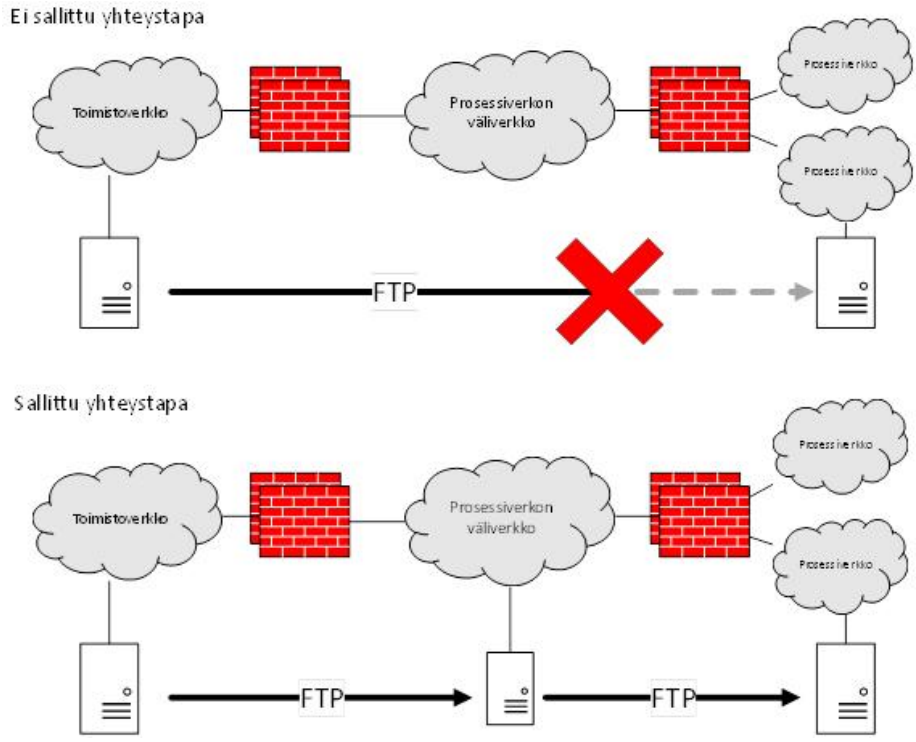
Yrityksen toimistoverkko on jaettu kolmeen alueeseen, jotka ovat palvelinverkko, runkoverkko sekä liityntäverkko. Toimistoverkossa on yrityksen IT-järjestelmiin liittyvät palvelimet ja niiden käyttöön liittyvät laitteet, kuten toimistotyöntekijöiden toimistotyöasemat sekä muut loppukäyttäjälaitteet, kuten tulostimet, IP-puhelimet sekä langattomat päätelaitteet. Palvelimet ovat toimistoverkon palvelinverkkovyöhykkeellä, jonka runkoverkko yhdistää liityntäverkkoon kytkettyihin työasemiin. Yrityksen internetliittymä on kahdennettu kahden eri operaattorin avulla.

Toimistoverkko on laajentunut aina uusien tarpeiden mukaisesti, ja se kattaa kaikki toimistorakennukset ja tehtaiden toimistotilat. Tehtaiden toimistotilojen lisäksi toimistoverkko on toteutettu muutamiin prosessikohteisiin erityistarpeiden vuoksi.

3.6.3 Prosessiverkon väliverkko

Prosessiverkon väliverkko toimii edustaverkkona prosessiverkon sisäänpäin ja ulospäin kulkeville yhteyksille. Yrityksen tietoturvaperiaatteiden mukaan suoria yhteyksiä prosessiverkon ja muiden verkkojen välillä ei sallita, vaan kaikki yhteydet tulee pysähtyä väliverkossa. Esimerkiksi suora FTP-tiedostonsiirto prosessiverkosta toimistoverkkoon ei ole sallittu, vaan yhteys pitää esimerkiksi päättää väliverkon FTP-palvelimelle, josta se

uudella ohjelmalla siirretään lopulliseen kohteeseen. Väliverkon palvelimilla ajetaan myös haittaohjelmantorjuntaa, mikä osaltaan lisää monikerroksisen verkkomallin suojausta. Sallittu ja kielletty tiedonsiirtotapa on esitetty kuvassa 2.



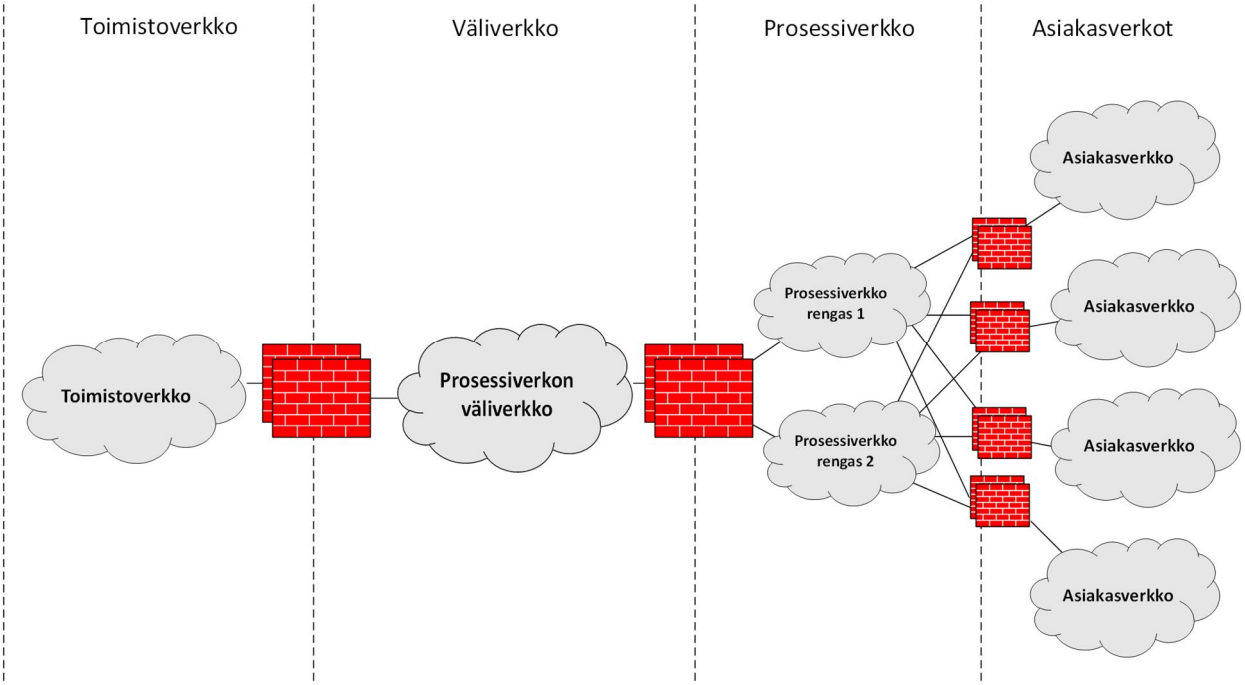
Kuva 2. Tiedonsiirtotapa yrityksen prosessiverkossa.

Väliverkko on erillinen L2-verkko, joka on hajautettu kahteen eri konesaliin. Näissä konesaleissa sijaitsevat prosessiverkon solmupisteet, kuten myös prosessiverkon pääpalomuurit. Pääpalomuurit yhdistävät toimistoverkon, prosessiverkon väliverkon sekä itse prosessiverkot.

3.6.4 Prosessiverkko

Prosessiverkko koostuu kahdesta erillisestä, toisistaan riippumattomasta rengasverkosta, jotka on kytketty kahdeksikon muotoon. Prosessijärjestelmien laitteet kuten alaasemat, mittalaitteet ja toimilaitteet kytketään jompaankumpaan rengasverkkoon. Järjestelmät ja laitteet erotellaan toisistaan VLAN-tekniikalla. Prosessiverkon yhteiskäyttöiset palvelut kuten aikasynkronointi, käyttäjätunnistus ja muut keskeiset infrapalvelut on hajautettu kumpaankin rengasverkkoon. Rengasverkot liittyvät muihin verkkoihin verkon solmupisteissä, prosessiverkon pääpalomuurien avulla.

Asiakasverkot on kytketty kumpaankin rengasverkkoon palomuurilaittein. Tällä saavutetaan mahdollisimman vikasietoinen tietoliikenneyhteys asiakasjärjestelmä ←→ asiakasjärjestelmä, ihminen → asiakasjärjestelmä kuten myös asiakasjärjestelmä ←→ ulkoinen järjestelmä välillä.



Kuva 3. Yrityksen verkkoarkkitehtuuri yleisesti.

3.6.5 Asiakasverkot

Asiakasverkot ovat joko yrityksen ICT:n, liiketoiminnon tai kolmannen osapuolen ylläpidossa. Asiakasjärjestelmät liittyvät asiakaskohtaisiin asiakaspalomuuriklustereihin joko access- tai trunk-tyyppisesti. Asiakasverkoissa käytetään joko ICT:n tai liiketoiminnon omia palvelimia ja päätelaitteita. Asiakasverkoista ei ole yhteyksiä yrityksen muihin verkkoihin tai internetiin.

3.7 Tiedonsiirto kuparikaapelissa

Kuparikaapelissa tietoa siirretään tyypillisesti kierretyssä parikaapelissa, jossa signaalijohtimien lähettävä ja vastaanottava johdin on kierretty keskenään. Parikaapelointijärjestelmästä riippuen kierrettyjä pareja on kaapelissa yhdestä kahdeksaan kappaletta.

Yksiparisia kuparikaapeleita eli puhelinkaapeleita käytetään nykyisin vain joissakin modeemiyhteyksissä, jossa tietoa siirretään hyvin pienellä nopeudella. Nykyisin asennettavat järjestelmät ovat joko CAT 6- tai CAT 7 -tyyppisiä, jotka pystyvät jopa 10Gb:n nopeuksiin. [Granlund 2007: 14.]

Kohdeyrityksellä on kiinteistöissä sisäinen CAT 6- tai CAT 7-yleiskaapelointijärjestelmä, joka mahdollistaa laitteiden liittämisen tietoliikennekytkimiin.

Kuparikaapelit ovat herkkiä sähkömagneettiselle säteilylle, mikä voi aiheuttaa häiriöitä ja haitata tiedonsiirtoa. Etenkin teollisuudessa, isot sähkökaapelit sekä muuntajat voivat häiritä kuparikaapeleissa tapahtuvaa tiedonsiirtoa.

3.8 Optinen tiedonsiirto

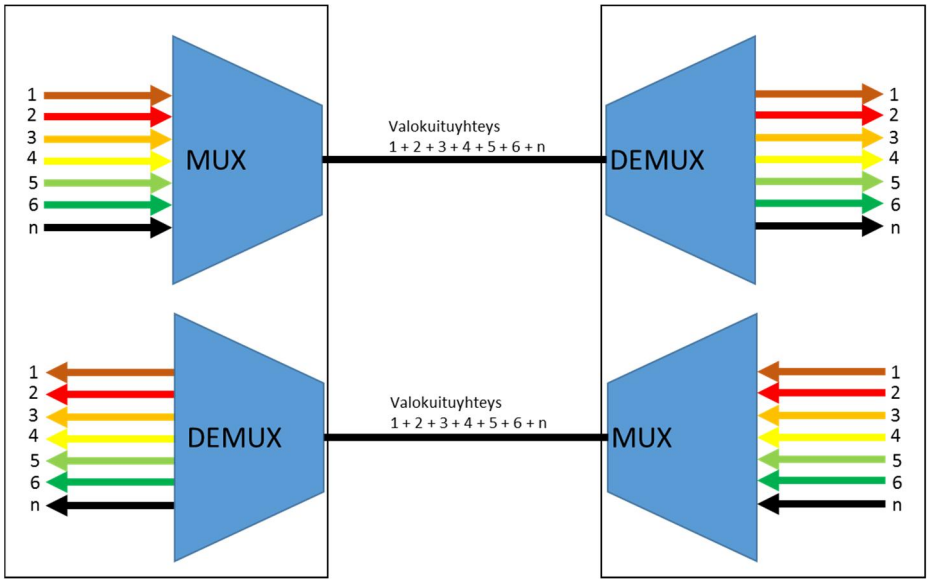
Valokuituyhteydet ovat optisia tiedonsiirtoyhteyksiä, joissa tietoa siirretään optisessa tiedonsiirtokaapelissa valopulsseina lähettimestä vastaanottimeen. Lähetin muuntaa lähetettävän tiedon eli datan valoksi, lähetettäväksi optiseen tiedonsiirtokaapeliin. Kaapelin toisessa päässä vastaanotin muuntaa valon jälleen dataksi. Optisissa yhteyksissä ei esiinny sähköisille signaaleille tyypillisiä häiriöitä, vaan lähes ainoita ongelmia ovat dispersio ja vaimennus.

Valokuituyhteydet ovat tekniikaltaan joko monimuotoisia tai yksimuotoisia. Monimuotoisessa valokuidussa voidaan käyttää LED- tai LASER-lähettimiä eivätkä yhteydet voi olla yhtä pitkiä kuin yksimuodossa, mikä johtuu siirrettävän valon dispersiosta eli valopulssin leviämisestä aikatasossa. Yksimuotoisissa yhteyksissä ei juuri esiinny dispersiota, sillä siinä valo pakotetaan kulkemaan heijastumatta kaapelin päästä päähän. Yksimuotokaapeleilla toteutetut yhteydet voivat olla kymmenien kilometrien pituisia, ja niissä voidaan käyttää myös aallonpituuskanavointia joka lisää kaapelin siirtokapasiteettia loogisten yhteyksien suhteen. [Granlund 2007: 14.]

Aallonpituuskanavoinnissa on kyse useamman eri aallonpituuden siirtämisestä samassa valokuitukaapelissa. Näitä järjestelmiä kutsutaan WDM-järjestelmiksi (Wavelength Division Multiplex). [Virtanen 2013: 15.] Optisissa tiedonsiirtokaapeleissa käytetään kolmea eri taajuusaluetta, jotka määräytyvät lasin ominaisuuksien mukaan. Käytettävät taajuusalueet ovat 825-875 nm, 1270-1340 nm ja 1525-1575 nm.

WDM-järjestelmiä on olemassa passiivisia, jossa eri yhteyksien aallonpituudet on valmiiksi sovitettu yhteysvälille, sekä aktiivisia, jossa aallonpituudet muutetaan sähköisesti yhteysvälille sopivaksi. Yrityksellä on käytössä vain passiivista WDM-tekniikkaa, minkä vuoksi tässä työssä ei käsitellä aktiivisia ratkaisuja.

WDM-järjestelmä koostuu lähettävän pään multiplekseristä, joka yhdistää usean valokuituyhteyden eri aallonpituudet yhteen valokuituyhteyteen sekä vastaanottavan pään multiplekseristä, joka jakaa eri aallonpituudet erillisille fyysisille kuituyhteyksille. WDM-laitteissa on käytännössä lähettävä ja vastaanottava multiplekseristä samassa laitteessa. [Virtanen 2013: 15.] WDM-järjestelmän toiminta on esitetty kuvassa 4.

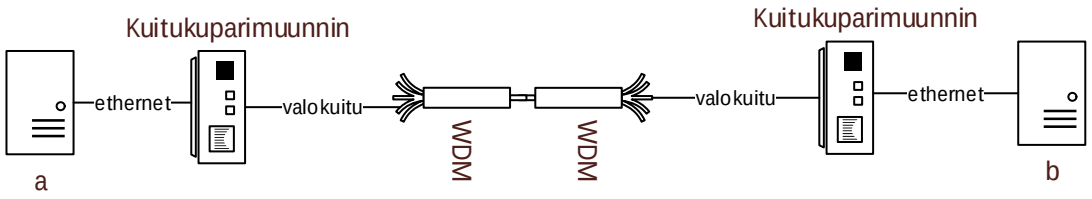


Kuva 4. WDM-järjestelmän toiminta.

Kohdeyrityksellä on kaikki toimipisteet kattava yksimuotoinen sekä kiinteistöissä sisäinen yksi- ja monimuotoinen valokuituverkko.

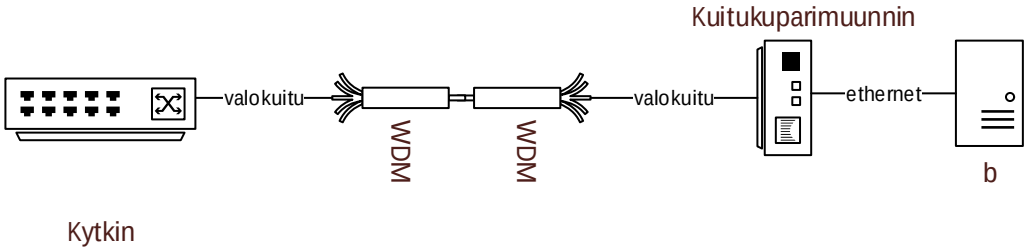
3.9 Valokuitu-ethernet-muuntimet

Valokuitu-ethernet-muuntimella ethernet-yhteys voidaan viedä pitkän matkan päähän valokuitua pitkin. Yhteyden kumpaankin päähän asennetaan muunninlaite ja yhteysvälille sopivat valokuitumoduulit, jotka muuntavat sähköisen tietoliikenteen valoksi, siirtävät sen valokuidulla ja muuttavat jälleen sähköksi. Tällainen yhteys on esitetty kuvassa 5.



Kuva 5. Valokuitu-ethernet-muuntimilla toteutettu yhteys

Valokuitu-ethernet-muunnin voidaan asentaa myös siten, että muunnin on yhteyden toisessa päässä ja toinen pää tietoliikennekytkimessä valokuituportissa. Tällöin tietoliikennekytkimen on oltava yhteensopiva käytetyn valokuitutekniikan kanssa. Tällainen yhteys on esitetty kuvassa 6.

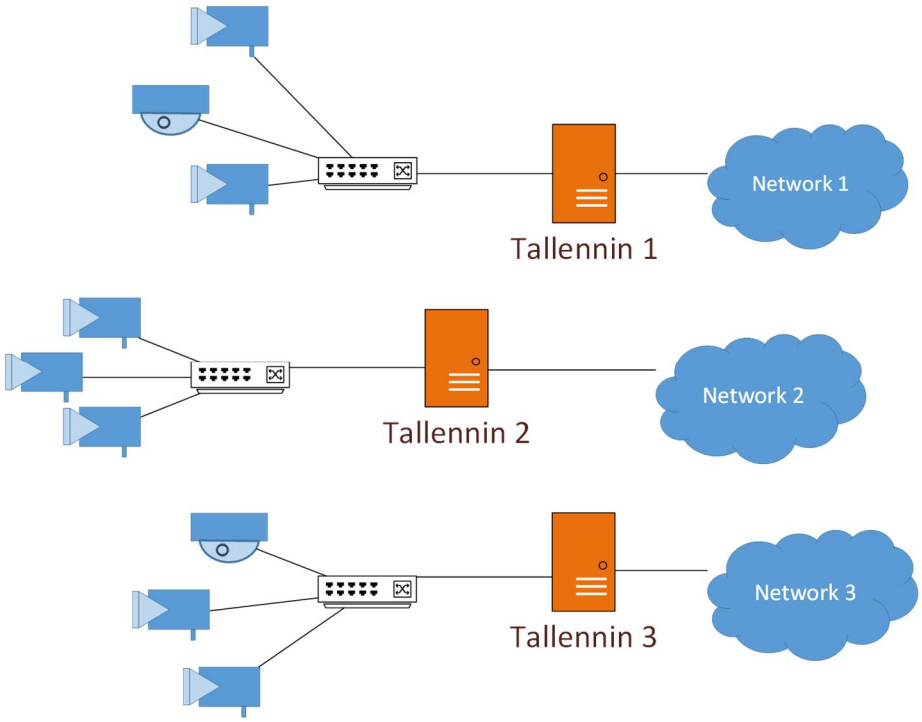


Kuva 6. Valokuitu-ethernet-muuntimilla toteutettu yhteys jossa yhteyden toisessa päässä kytkinlaite.

3.10 Kamerajärjestelmät

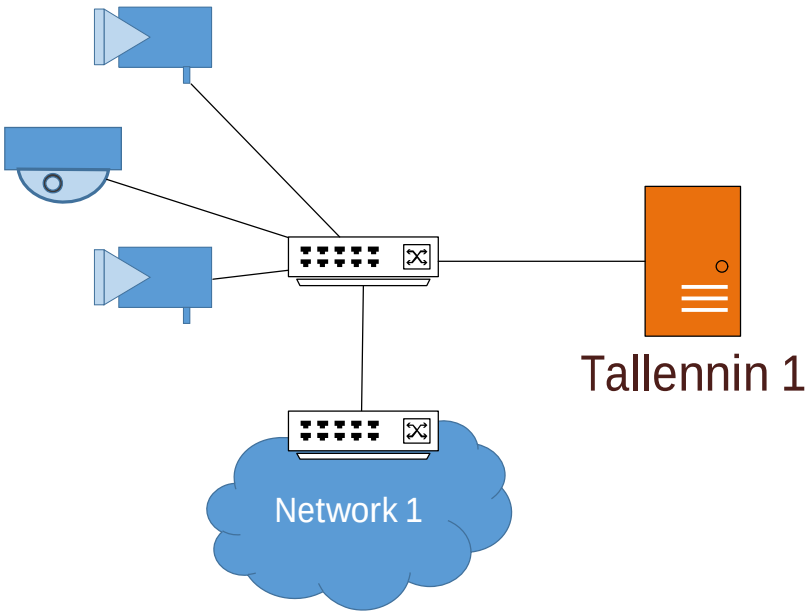
Yrityksellä on käytössä neljäkymmentäkolme kamerajärjestelmää, jotka ovat tietoliikenneteknisesti sijoitettu toimistoverkkoon, prosessiverkkoon ja asiakasverkkoihin. Toimistoverkkoon on kytketty yhdeksän järjestelmää, prosessiverkkoon kolmekymmentäneljä, joista kolme on asiakasverkon ja loput runkoverkon puolella.

Käytössä olevista järjestelmistä osalla valvotaan turvallisuutta ja osalla tuotantoprosessien toimintaa. Kameravalvontajärjestelmät on toteutettu siten, että jokaisella lämpölaitoksella, voimalaitoksella, sähköasemalla tai toimistokiinteistöllä on oma paikallinen kameratallennin sekä kameraverkko. Järjestelmät ovat voimalaitosjärjestelmiä lukuun ottamatta niin sanotusti dual-host -tyyppisiä (kuva 7), jolloin kamerat ovat paikallisessa L2-kameraverkossa ja tallennin kytketty sekä kameraverkkoon että yrityksen verkkoon.



Kuva 7. Dual-host -tyyppisten kameravalvontajärjestelmien kytkentä ulkoisiin verkkoihin.

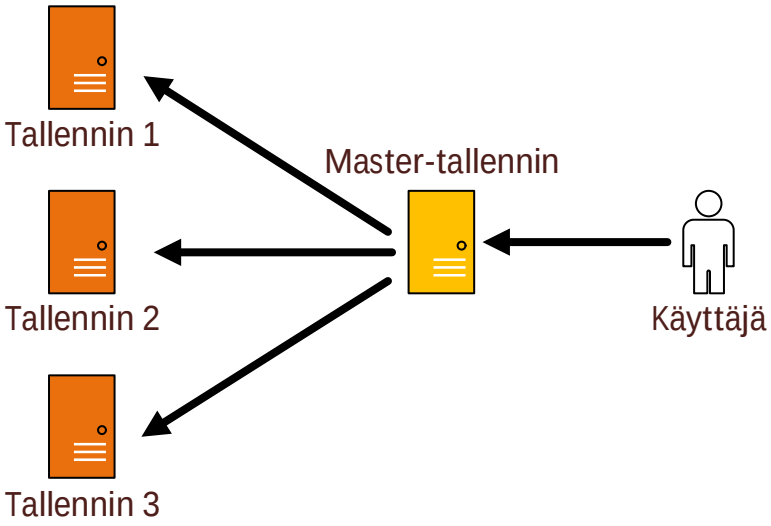
Voimalaitoskamerajärjestelmät ei ole kytketty dual-host -tavalla, vaan tallentimet ja kamerat on kytketty L2-verkkoon, joka on kytketty access-yhteytenä yrityksen verkkoon.



Kuva 8. Kameravalvontajärjestelmän kytkentä ulkoiseen verkkoon L2-tasoisesti.

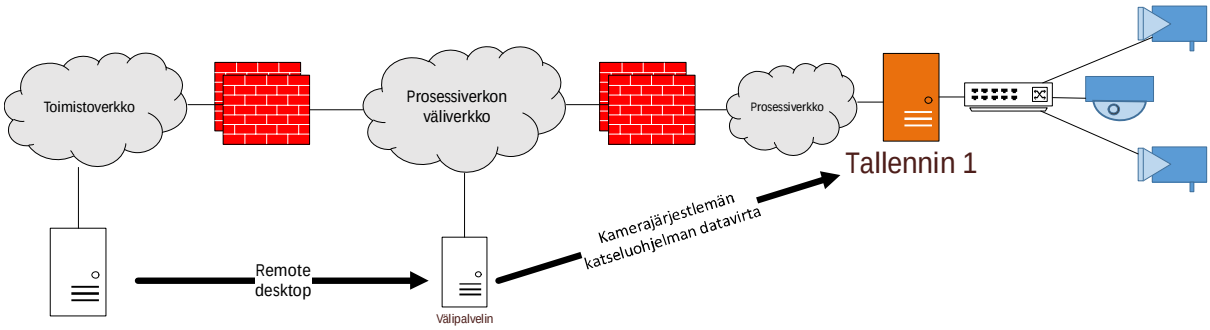
Kameroiden etäkäyttö tapahtuu aina etäyhteyden, master-tallentimen tai katseluohjelman avulla. Katseluohjelma ottaa yhteyden kameratallentimen ohjelmistoon, joka välittää pakatun kameradatan verkon avulla katseluohjelmalle.

Master-tallentimet ovat kerääviä videotallentimia, jotka eivät ole yhteydessä kameroihin vaan toisiin tallentimiin. Master-tallentimien avulla voidaan keskitetysti hallita laitosten ja kiinteistöjen tallentimien asetuksia ja loppukäyttäjien käyttöoikeuksia. Master-tallennin myös kerää ja tallentaa videodatan toisista tallentimista (kuva 9).



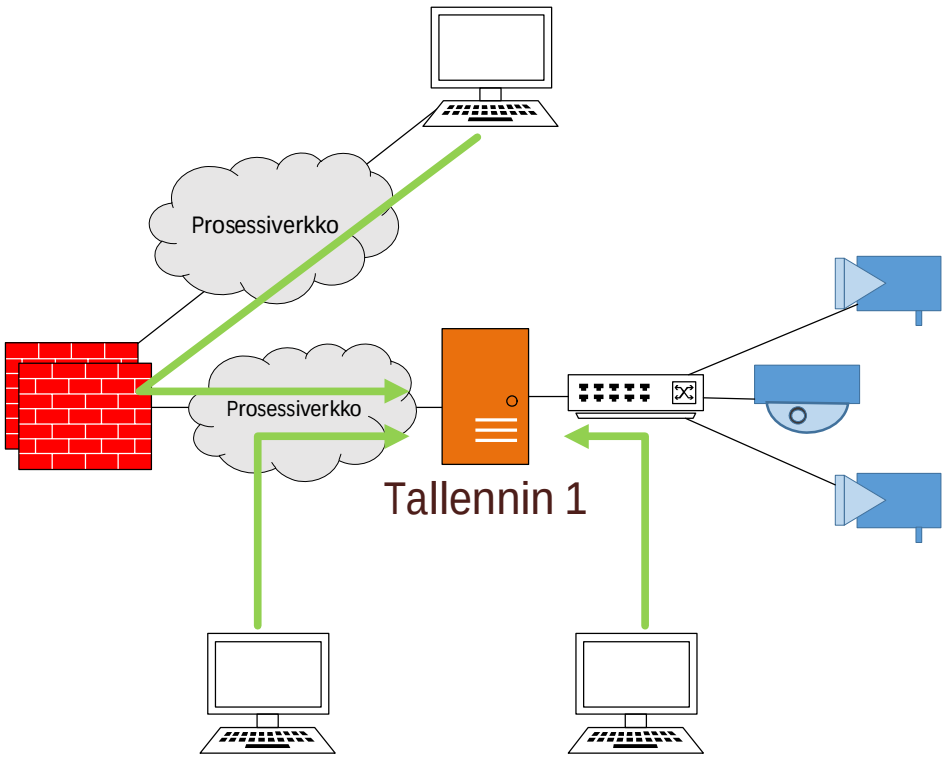
Kuva 9. Usean tallentimen etäkäyttö master-tallentimen kautta.

Toimistoverkossa olevia kamerajärjestelmiä käytetään toimistotyöasemilla etäyhteyden kautta tai paikallisella katseluohjelmistolla. Prosessiverkkoon ja asiakasverkkoihin sijoitettuihin kamerajärjestelmiin ei yrityksen tietoturvaperiaatteiden vuoksi voi avata suoraan etäyhteyttä, vaan yhteys on otettava prosessiverkon välipalvelimen kautta.



Kuva 10. Kameravalvontajärjestelmän etäkäyttö yrityksen toimistoverkosta.

Kamerajärjestelmien tehokäyttöä varten prosessiverkkoon ja asiakasverkkoihin on sijoitettu työasemia, joilla voidaan avata suoria katseluyhteyksiä kamerajärjestelmiin.



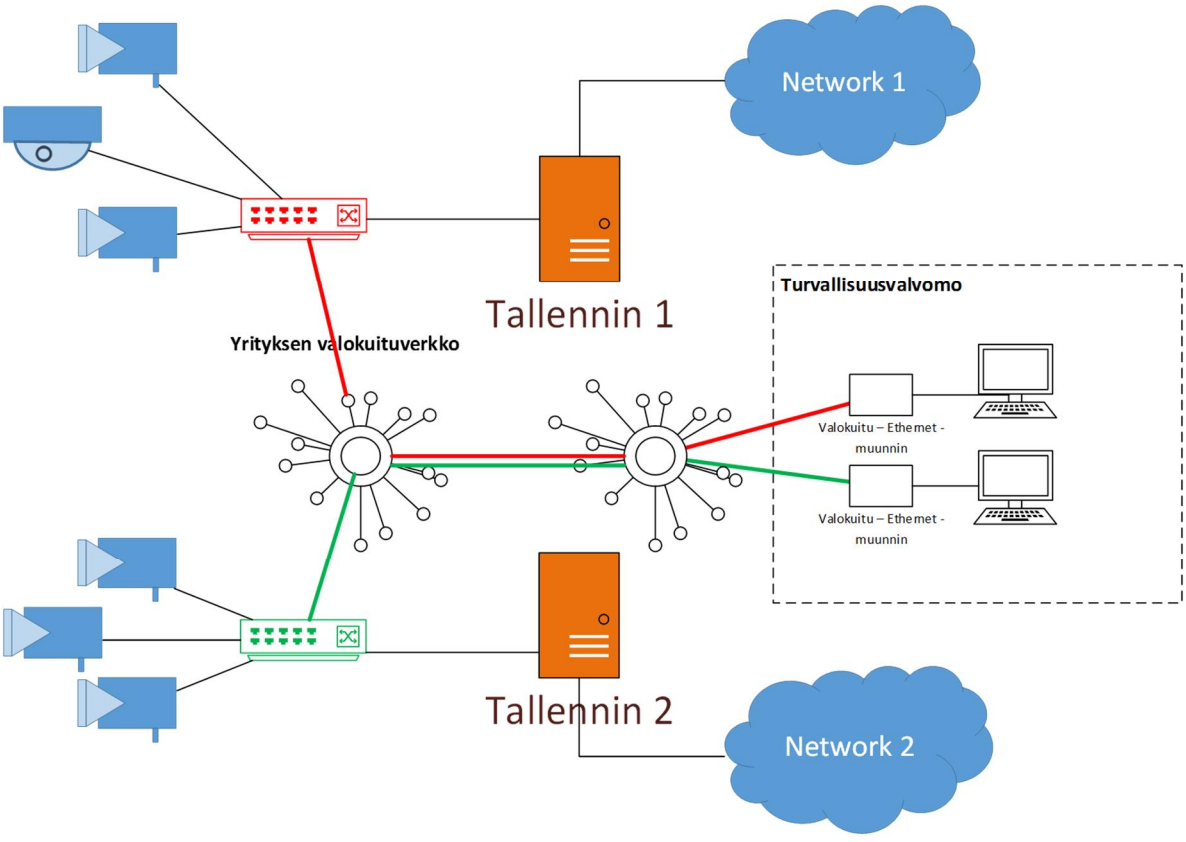
Kuva 11. Kameravalvontajärjestelmän etäkäyttö prosessiverkon ja paikallisen kameraverkon kautta.

3.11 Nykyisen arkkitehtuurin haasteet

Nykyiset kytkinverkot ja palomuurilaitteet ovat nopeudeltaan 1Gb/s. Prosessiverkko ja osa asiakasverkoista on jaettu muiden järjestelmien kesken. Monet verkoissa käytettävät tietoliikenneprotokollat ja sovellukset on alun perin suunniteltu sarjaliikenneväyliin, joissa ei käytännössä esiinny kulkuaikaviivettä. Nämä protokollat on myöhemmin muokattu TCP/IP-protokollapinon päälle muuttamatta niitä käyttäviä sovelluksia riittävästi. Esimerkkinä tällaisesta protokollasta voidaan mainita ANSI C -protokolla, jolla siirretään sarjaliikennesanomia TCP/IP:n päällä. Sarjaliikennepohjainen historia aiheuttaa sen, että sovellukset ja protokollat eivät välttämättä kestä suurta kulkuaikaviivettä (delay) tai sen vaihtelua (jitter).

Koska kamerajärjestelmät on kytketty toimistoverkkoon, prosessiverkkoon sekä asiakasverkkoihin, aiheuttaa niiden etäkatselu huomattavaa verkkoliikennettä jaettuihin palo-

muureihin ja kytkinverkkoihin. Tällainen verkkoliikenne saattaa häiritä kulkuaikaviivekriittisten sovellusten toimintaa ja näin haitata yrityksen liiketoimintajärjestelmien käyttöä. Häiriöiden minimoimiseksi kytkinportit, joissa kameravalvontajärjestelmät on kytketty, on rajoitettu toimimaan 100 Mb:n nopeudella. Tällä konfiguraatiolla kamerajärjestelmät saadaan toimimaan paikallisesti tehokkaasti mutta samalla varmistetaan, että etä-käyttö ja -katselu ei kuormita tietoliikenneverkkoa liikaa. Tämän rajoituksen vuoksi yrityksen keskitettyyn turvallisuusvalvomoon ei voi tehokkaasti tuoda videokuvaa jaetun kytkinverkon kautta, vaan tätä varten on toteutettu suoria kuituyhteyksiä. Suorat kuituyhteydet on toteutettu kameravalvontajärjestelmien sisäverkosta tuomalla katselutyöasemia turvallisuusvalvomoon. Yhteydet on toteutettu valokuitu-ethernet-muuntimilla, jotka mahdollistavat ethernet-yhteyksien tuomisen pitkän matkan päähän. Valokuitumuunnin muuntaa ethernet-kupariyhteyden valoksi, ja päinvastoin.



Kuva 12. Kamerajärjestelmien etäkatselutyöasemien verkkoyhteyden järjestäminen yrityksen valokuituverkon kautta.

4 Runkoverkon suunnittelu

Kameravalvontajärjestelmien runkoverkon suunnittelussa pyritään ratkaisuun, jossa ei ole nykyisen arkkitehtuurin rajoituksia. Eri toimitilojen ja laitosten kameravalvontajärjestelmät tulee pystyä liittämään verkkoon kustannustehokkaasti ja riittävällä vikasietoisuudella.

Videodatan siirtäminen kameraverkossa ei saa häiritä muiden tietojärjestelmien toimintaa. Runkoverkon runkoyhteyksien tulee olla riittävän suorituskykyisiä, jotta järjestelmien etäkatselu on mahdollista myös runkoverkon kautta.

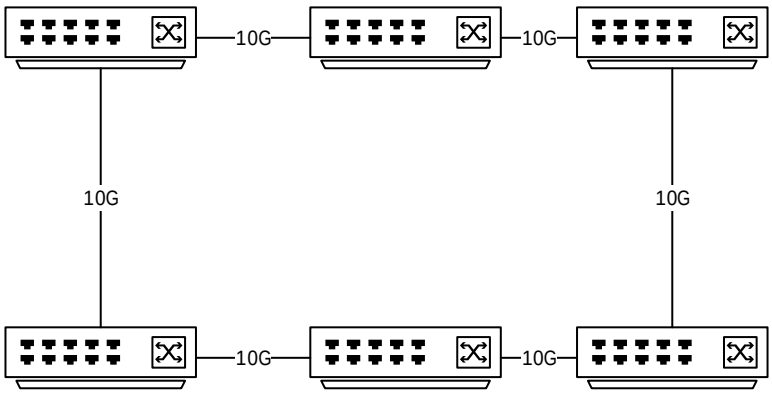
4.1 Runkoverkon kytkinarkkitehtuuri

Koska runkoverkkoon liitettäviä kameravalvontajärjestelmiä on kymmenissä toimipisteissä, mutta toimipistekohtaisesti järjestelmiä on pääosin yksi tai enintään muutama, ei ole kustannustehokasta asentaa kameravalvontaverkon kytkinlaitetta jokaiseen toimipisteeseen. Yrityksellä on käytössä laaja valokuituverkko, joka kattaa kaikki toimipisteet. Valokuituverkossa on useita solmupisteitä, joiden kautta yhteyksiä voidaan ristikytkeä.

Verkko voidaan toteuttaa rengasverkkona, jolloin verkon kytkimet on kytketty renkaan muotoon, tai tähtiverkkona, jolloin tietyt kytkimet toimivat niin sanottuina keräävinä kytkiminä, joihin toimipisteiden kytkimet kytketään.

Yrityksen valokuituverkko on rengasmainen, sillä se koostuu useista renkaan muotoon asennetuista runkoyhteyksistä. Rengasverkkoja täydentävät oksamaiset yhteydet, jotka ulottuvat etäisiin kohteisiin. Valokuituverkon rakenteen vuoksi runkoverkko on järkevää toteuttaa rengasmaisena. Runkoverkon kytkimet hankitaan ja asennetaan valokuituverkon kannalta tehokkaisiin solmupisteisiin. Koska runkoyhteyksien kautta siirretään runsaasti videodataa, on runkoyhteydet (uplink) syytä toteuttaa 10 Gb:n nopeuksilla.

Runkoverkon kytkinlaitteiden yleisarkkitehtuuri on esitetty kuvassa 13.



Kuva 13. Rengas-tyyppinen kameravalvontajärjestelmien runkoverkko.

Kytkinlaitteiden asennuskohteissa on usein saatavilla varmennettua sähköä yksi tai kaksisyöttöisenä. Runkokytkimet on syytä hankkia kahdennetulla sähkönsyötöllä, jotta yhden sähkönsyötön vikaantuminen ei lopeta laitteen toimintaa, vaan laite pysyy käynnissä yhden sähkönsyötön avulla, kunnes toinenkin sähkönsyöttö on korjattu. Kohteissa, joissa on vain yksi varmennettu sähkönsyöttö, voidaan toinen sähkönsyöttö ottaa suoraan varmentamattomasta sähköverkosta.

Tietoliikennelaitteet voidaan sijoittaa yrityksen prosessiverkon tietoliikennekaappeihin, sillä ne ovat jo valmiiksi yrityksen periaatteiden mukaisesti asennettuja ja lukittuja. Kaapit ovat RITTAL:n umpikaappeja mallimerkinnältään 5834.500. Kaapin mitat ovat 800x600x2000 mm (leveys x syvyys x korkeus), jolloin asennettavan laitteen suurin syvyys on enintään 524 mm. [Kytkentäkaapit 2018: 16.]

4.2 Tietoliikenteen eristäminen verkossa

Eri järjestelmien tietoliikenne eriytetään runkoverkossa IEEE 802.1Q -virtuaalilähiverkko tekniikalla (VLAN). Käytettäessä VLAN:ja, ethernet -verkot jaetaan loogisiin osiin, jossa verkon kytkimet ja reitittimet välittävät tietoliikennepaketteja vain kunkin verkon sisällä. Liikenne VLAN:ien välillä tapahtuu aina reitittävän laitteen kautta, joka voi olla myös palomuuri. Käytettäessä VLAN-tekniikkaa verkkolaitteet lisäävät ethernet-paketeihin 802.1Q kehyksen, jonka hyötykuormaksi merkitään tieto siitä, mihin VLAN:iin kyseinen tietoliikennepaketti kuuluu. Merkityistä paketeista käytetään nimitystä tagged. Merkittyjä

paketteja välitetään vain verkon trunk-yhteyksissä, sillä tällöin yhteyden kummassakin päässä on laite, joka tukee kyseistä protokollaa. Normaali työasema, joka ei välttämättä tue VLAN-tekniikkaa, liitetään verkossa aina access-porttiin. Access-porttiin ei lähetetä VLAN-merkittyjä tietoliikennepaketteja, vaan 802.1Q -kehys poistetaan ennen päätelaitteelle lähetystä. Tällöin paketti on niin sanotusti untagged. Mikäli päätelaite liikennöi verkkoon access-portissa, lisää tietoliikennekytkin tähän VLAN-merkinnän ennen kuin se välitetään eteenpäin. [VLANs and Trunking: 17.]

Runkoverkon kytkimet kytketään toisiinsa trunk-tyyppisesti, jolloin kaikki tietoliikennepaketit ovat VLAN-merkittyjä, minkä perusteella tiedetään, mihin verkkoon kyseinen tietoliikennepaketti kuuluu. Kameravalvontajärjestelmien ei tarvitse tukea VLAN-tekniikkaa, koska järjestelmät kytketään kytkinten access-portteihin. Kytkimen access-portti lähettää ja vastaanottaa tietoliikennepaketteja, joissa ei ole VLAN-merkintää.

Yrityksen tietoturvaperiaatteiden mukaan VLAN-tekniikan turvallisuuteen ja eriyttämiseen luotetaan prosessiverkkokäytössä, mutta samaa layer 2 -tason verkkoa ei saa käyttää muuhun tarkoitukseen, kuten esimerkiksi toimistoverkon, prosessiverkon väliverkon tai muiden verkkojen siirtämiseen.

4.3 Layer 2 -hallintaprotokolla

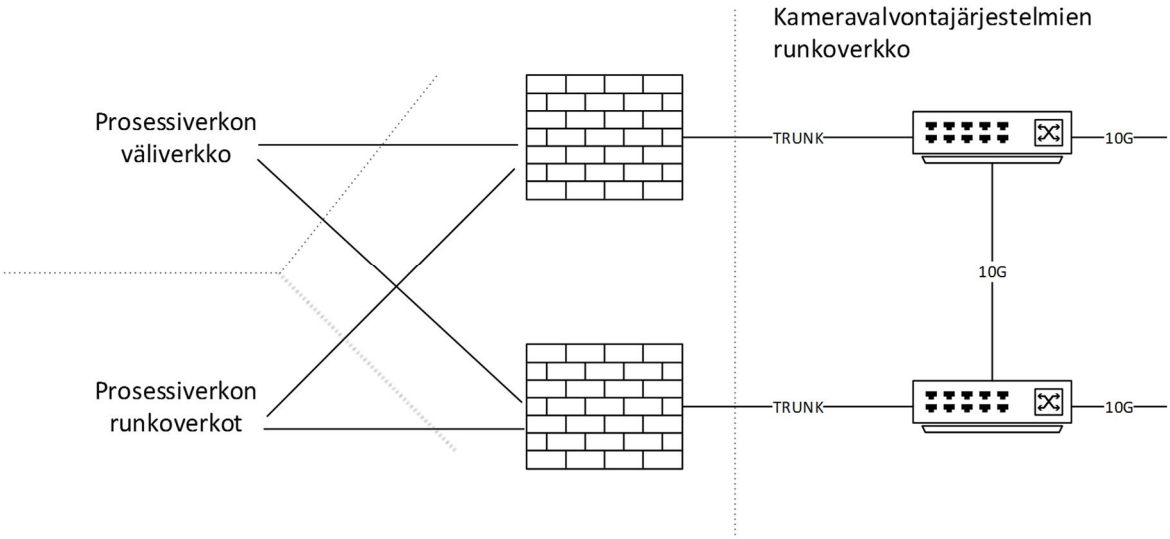
Layer 2 -hallintaprotokollan tarkoituksena on hallinnoida kytkinlaitteiden layer 2 -topologiaa ja estää datanvälityssilmukoiden syntyminen. Ilman topologianhallintaa verkossa muodostuisi yksi tai useampi silmukka, joka välittäisi tietoliikennepaketteja loputtomasti eteenpäin, lopulta tukkien koko verkon. Rengasverkkoa ei olisi mahdollista tehdä ilman tällaista hallintaprotokollaa. Hallintaprotokollan avulla verkon kytkimet muodostavat vikasietoiset kytkentäreitit, mikäli jokin yhteysväli katkeaa. [Äikäs 2015: 18.]

Layer 2 -hallintaprotokollia on olemassa useita, jotka on suunniteltu eri käyttötarkoituksiin. Kameravalvontajärjestelmien runkoverkkoon valitaan yksinkertainen spanning tree -protokolla sen yksinkertaisuuden vuoksi, ja koska sitä käytetään myös yrityksen muissa verkoissa. Spanning tree -protokollasta on olemassa useita eri versioita: osa vanhempia ja osa nykyaikaisempia, jotka toimivat vain tiettyjen laitevalmistajien laitteissa. Yrityksen kytkinlaitteet ovat CISCO:n valmistamia, minkä vuoksi myös nyt suunniteltavassa verkossa on järkevää käyttää CISCO:n laitteita. CISCO:lla on spanning tree -protokollasta

olemassa per VLAN spanning tree plus -versio (PVST+) jossa layer 2 -topologia neuvotellaan VLAN-kohtaisesti. PVST+:aa käytettäessä kytkinten kytkentälinkeille muodostuu eräänlaista kuormantasausta, kun verkko katkaistaan VLAN-kohtaisesti fyysisen kytkinverkon eri kohdista.

4.4 Kytkentä muihin verkkoihin ja reititys

Tietoliikennerunkoverkon eri VLAN:n sekä muiden verkojen välillä tapahtuu aina reititysprosessin kautta. Reititysprosessia suoritetaan prosessiverkon palomuurilaitteissa, joihin runkoverkko on kytketty. Palomuurilaitteet sijaitsevat rungon solmupisteissä joihin myös kameravalvontajärjestelmien runkoverkon kytkimet kytketään.



Kuva 14. Kameravalvontajärjestelmien uuden runkoverkon kytkentä muihin verkkoihin.

Prosessiverkon palomuurilaitteissa käytetään dynaamista OSPF-reititysprotokollaa, joka mainostaa palomuuriin kytketyt kameravalvontajärjestelmät yrityksen ylemmän tason reitityskerroksille.

OSPF on dynaaminen reititysprotokolla, joka jakaa reititystietoa reititettävistä protokollista kuten IP:stä. [Wikipedia 2018: 19.] OSPF:n avulla palomuurilaitteet mainostavat toisille samalla reititysalueella oleville reitittimille ja palomuureille itseensä kytketyt verkot, ja tarvittaessa myös muiden reititysprosessien kautta tuodut reititystiedot. Reititysprotokollan avulla verkon reitityksen ylläpito yksinkertaistuu, kun kaikkia reititystietoja ei tarvitse määritellä käsin kaikille verkon laitteille.

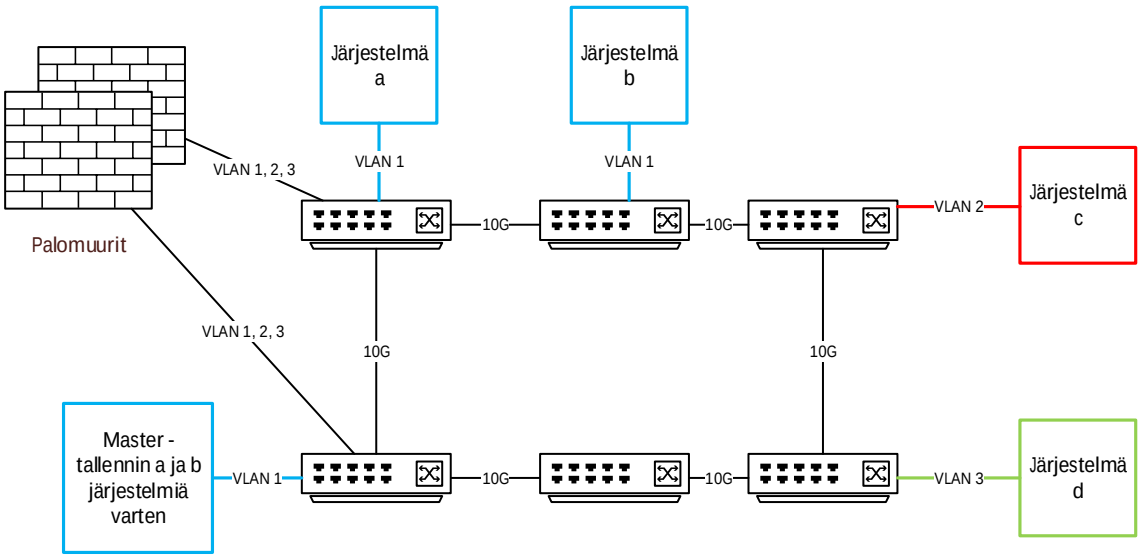
4.5 Verkon valvonta

Verkon aktiivilaitteet liitetään yrityksen prosessiverkkoympäristön keskitettyyn verkonvalvontaan. Valvonta on toteutettu Ciscoworks LMS -tuotteella, joka on CISCO:n tietoliikenneverkon hallinta- ja valvontajärjestelmä (NMS).

Ciscoworks valvoo verkon aktiivilaitteita SNMP-protokollalla sekä kirjautumalla SSH-yhteydellä laitteisiin ja keräämällä mm. lokitietoa. Ohjelmistoon voidaan konfiguroida valvontanäkymiä ja sähköpostihälytyksiä, joiden avulla verkon tilaa on mahdollista seurata. Ohjelmisto kerää myös monipuolisesti suorituskykydataa verkon laitteista, jonka avulla voidaan tunnistaa ja ennakoida vikatilanteiden syntymistä.

4.6 Verkkoliikenteen suodatus

Kaikki liikenne kameravalvontajärjestelmien sekä muiden järjestelmien välillä kulkee aina prosessiverkon palomuurien kautta. Palomuurit määritellään siten, että kaikki tietoliikenne on oletuksena estetty, ja vain tarvittavat yhteydet sallitaan. Kameravalvontajärjestelmät, jotka kerätään saman master-tallentimen piiriin, sijoitetaan samaan aliverkkoon, jotta videokuvavirta ei rasittaisi liikaa jaettuja palomuureja.

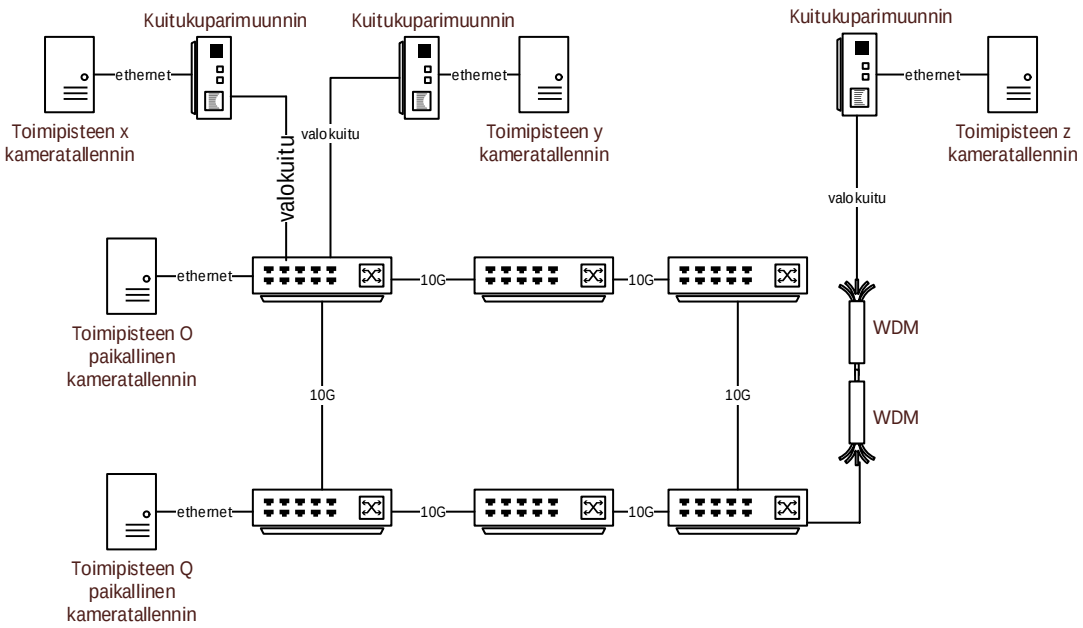


Kuva 15. Kameravalvontajärjestelmien verkkoliikenteen soudatus ja eriyttäminen VLAN-tekniikalla.

4.7 Kameravalvontajärjestelmien liityntä runkoverkkoon

Kameravalvontajärjestelmät liittyvät runkoverkkoon access-tyyppisesti. Yrityksellä käytössä olevien kameravalvontajärjestelmien tallentimet on varustettu yhdellä tai kahdella verkkokortilla. Yhden verkkokortin tallennin liitetään runkoverkon kytkimeen yhdellä yhteydellä jolloin liityntä ei ole vikasietoinen. Kahdennetulla verkkokortilla varustetut tallentimet voidaan liittää yhteen tai kahteen kytkimeen.

Koska runkoverkon kytkimet hankitaan vain valokuituverkon solmupisteisiin, täytyy muissa kohteissa olevien tallentimien yhteydet tuoda ethernet-valokuitumuuntimilla. Runkoverkon kytkimiksi hankitaan niin sanottuja kuitukytkimiä, jotka varustetaan valokuitumoduuleilla, mitkä ovat yhteensopivia käytetyn kuitumuuntimen kanssa. Yhteysväleillä, joissa käytetään WDM-tekniikkaa, valokuitumoduuleiksi on valittava oikealla aallonpituudella toimivia kumpaankin päähän yhteyttä. Paikallisten ja etätallentimien kytkentäperiaate verkkoon on esitetty kuvassa 16.



Kuva 16. Kameravalvontajärjestelmien liityntä runkoverkkoon kytkentäkaapelilla ja valokuitu-ethernet -muuntimilla.

Kameravalvontajärjestelmät liitetään runkoverkkoon enintään 1 Gbps:n nopeudella, jotta runkoverkon 10 Gbps:n kapasiteetti riittää kaikille järjestelmille.

4.8 Kytkinten vertailu ja valinta

Kuten luvussa 4.3 Layer 2 -hallintaprotokolla mainitaan, on yrityksen nykyiset tietoliikennekytkimet CICSO:n valmistamia, minkä vuoksi myös järjestelmien runkoverkkoon on syytä valita CISCO:n kytkimet. Tässä insinöörityössä kytkinten valinnalle on tunnistettu seuraavat vaatimukset:

- 10Gb:n uplink SFP -moduulipaikat
- VLAN-tuki
- kaksi sähkönsyöttöä
- SNMP tuki valvontaa varten
- liitännät valokuitumoduuleilla (SFP)
- suurin syvyys enintään 524 mm.

Vertailuun haettiin vaihtoehdot CISCO:n switch selector -työkalulla, joka tarjosi vaihtoehdoiksi Cisco Catalyst 3650-, 3850- ja 9300-tuoteperheitä. Kaikista tuoteperheistä oli saatavilla kytkinmallia, jossa on 10Gb:n uplink SFP -moduulipaikat mutta vain 3850-sarjasta löytyi kytkinmalli, jossa on laitteiden kytkentään SFP-moduulipaikat. Laitteiden vertailu on esitetty taulukossa 1.

Taulukko 1. Kytkinmallien vertailu

Kytkinmalli	Tuoteperhe	10 Gb SFP	1 Gb SFP	Muut moduulit
-	Cisco Catalyst 3650	-	-	-
WS-C3850-12S-S	Cisco Catalyst 3850	0	12	2 x 10 GE, 4 x 1 GE
WS-C3850-24S-S	Cisco Catalyst 3850	0	24	2 x 10 GE, 4 x 1 GE
-	Cisco Catalyst 9300	-	-	-

4.9 Runkoverkon kapasiteetti

Kameravalvontajärjestelmien runkoverkkoon tuottaman tietoliikenteen määrä riippuu etäkäyttäjien ja katseltavien kuvavirtojen sekä master-tallentimiin kytkettyjen tallentimien määrästä, kuten myös näissä käytetyistä videoprotokollista, joilla videon ääni ja kuva siirretään tietoliikenneverkossa. Videoprotokollissa käytetään videonpakkausta, jolla videokuva saadaan vähemmän tilaa vievään muotoon. [Wikipedia 2018. 19.] Yleisesti käytettyjä videopakkausprotokollia ovat Motion JPEG, MPEG-4 ja H.264, joka on viimeisin ja tehokkain protokolla. [Axis 2018: 29.] Videoprotokollien tarvitsema kaistanleveys on esitetty taulukossa 2.

Taulukko 2. Pakatun videokuvan vaatima kaistanleveys

	Pakkausprotokolla	
Resoluutio	H.264	MJPEG
1280*720	2 Mbps	6 Mbps
1920*1080	4 Mbps	12 Mbps
2560*1440	8 Mbps	24 Mbps

Runkoverkon kytkimet ovat runkoporttinopeudeltaan 10 Gb:ä, ja koska kameravalvontajärjestelmät liittyvät enintään 1 Gb:n nopeudella, riittää runkoverkko kameravalvontajärjestelmien liityntänopeuden osalta teoriassa vain kymmenelle kameravalvontajärjestelmälle. Käytännössä kameravalvontajärjestelmät eivät tuota 1 Gb:n verkkoliikennettä, vaan tietoliikenteen määrä on alhaisempi. Jos verkossa siirrettävässä videokuvassa käytetään H.264-protokollaa ja 1280*740-resoluutiota, riittää koko runkoverkon 10 Gbps:n kapasiteetti teoriassa 5000 samanaikaiselle kuvavirralle.

4.10 Runkoverkon fyysinen arkkitehtuuri

Runkoverkon fyysinen arkkitehtuuri on esitetty liitteessä 1, joka on määritelty salaiseksi.

5 Johtopäätökset ja yhteenveto

Työn tavoitteena oli selvittää kohdeyrityksen kameravalvontajärjestelmien nykyinen tietoliikennearkkitehtuuri ja käytännön haasteet, sekä suunnitella yrityksen tarpeet täyttävä runkoverkko kameravalvontajärjestelmille. Tavoitteet täyttyivät, sillä työn tuloksena syntyi selvitys nykyistä kameravalvontajärjestelmistä, nykyarkkitehtuurin haasteet tunnistettiin ja lopuksi kerätyn tiedon pohjalta suunniteltiin uusi runkoverkko. Lisäksi työssä tehtiin järjestelmien siirtoprojektia varten liityntätapakohtainen tietoliikennearkkitehtuurikuvaus, jossa käytettiin esimerkkinä yrityksen oikeita järjestelmiä.

Yritykselle pystyttiin suunnittelemaan kameravalvontajärjestelmien runkoverkko yllättävän pienellä tietoliikennekytkinmäärällä, mikä johtuu olemassa olevasta valokuitukapasiteetista. Mikäli valokuituyhteydet pitäisi ostaa vapailta markkinoilta, voisi olla järkevää ostaa enemmän kytkimiä ja minimoida näin käytettyjen kuituyhteyksien määrä.

Insinöörityön palautushetkellä uuden runkoverkon rakennusta ei ollut vielä aloitettu, mutta verkon toteutus budjetoitiin vuodelle 2019.

Yrityksen palautteen mukaan tämän insinöörityön pohjalta heillä on nyt riittävät tiedot uuden runkoverkon toteuttamiseksi. Lisäksi työssä tehdyt esimerkkisuunnitelmat helpottavat tietoliikennearkkitehtien työtä itse siirtoprojektissa.

Lähteet

1 Sallinen, Pekka. 2011. Kameravalvontaopas. Sähköinfo.

2 Real time streaming protocol. 1998. Verkkodokumentti. Internet Engineering Task Force https://tools.ietf.org/html/rfc2326. Viitattu 30.9.2018.

3 Koneoppimisen hyödyntäminen konenäössä. 2016. Verkkodokumentti. Kiesiläinen, Jarno. https://jyx.jyu.fi/handle/123456789/52738. Viitattu 30.9.2018.

4 Usein kysyttyä EU:n tietosuoja-asetuksesta. Verkkodokumentti. Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/gdpr. Viitattu 30.9.2018.

5 Laki yksityisyyden suojasta työelämässä 759/2004.

6 Laki yhteistoiminnasta yrityksissä 334/2007.

7 Mikä on tietoturvaloukkaus ja miten sellaisen sattuessa pitää toimia? Verkkodokumentti. Euroopan komissio https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_fi. Viitattu 25.8.2018.

8 Mitä on huoltovarmuus? Huoltovarmuuskeskus. Verkkodokumentti. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/mita-on-huoltovarmuus/. Viitattu 30.8.2018.

9 Tavoitteet. Huoltovarmuuskeskus. Verkkodokumentti. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/tavoitteet/. Viitattu 30.8.2018.

10 Operational Technology (OT). Gartner. Verkkodokumentti. https://www.gartner.com/it-glossary/operational-technology-ot/. Viitattu 30.8.2018.

11 Yrityksen prosessitietojärjestelmiä koskeva konserniohje. SALATTU.

12 Hakala Mika, Vainio Mika. 2005. Tietoverkon rakentaminen. Docendo.

13 Demilitarisoitu alue (tietotekniikka). Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/Demilitarisoitu_alue_(tietotekniikka). Viitattu 30.8.2018.

14 Granlund, Kaj. 2007. Tietoliikenne. Docendo.

15. Virtanen, Reijo. Sähköasemien tiedonsiirron kehittäminen Helen Sähköverkko Oy:ssä. 2013. Opinnäytetyö. http://urn.fi/URN:NBN:fi:amk-2013053112055.

16. Kytkentäkaapit. Rittal Oy. Verkkodokumentti. http://www.rittal.com/imf/none/3_4088/Rittal_5834500_Tekniset_erittelyt_3_4088. Viitattu 28.8.2018.

17 VLANs and Trunking. Cisco. Verkkodokumentti. http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3. Viitattu 28.8.2018.

18 Äikäs, Jussi. 2015. SPANNING TREE -PROTOKOLLAN TOIMINTA TIETOVERKOSSA. Opinnäytetyö. https://www.theseus.fi/bitstream/handle/10024/96063/Aikas_Jussi.pdf.

19 OSPF. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/OSPF. Viitattu 30.8.2018.

19 Videonpakkaus. Verkkodokumentti. Wikipedia. https://fi.wikipedia.org/wiki/Videonpakkaus. Viitattu 1.9.2018.

20 Video compressing. Verkkodokumentti. Wikipedia. https://www.axis.com/en-rs/learning/web-articles/technical-guide-to-network-video/video-compression-guide. Viitattu 1.9.2018.

Runkoverkon fyysinen ja maantieteellinen arkkitehtuuri

Liite salattu

Tietoliikennearkkitehtuurikuva: Kamerajärjestelmän siirtäminen prosessiverkosta kameraverkkoon

Liite salattu